ALGORITHM FOR RFID SECURITY

TECHNICAL FIELD

[0001] The invention relates to the use of radio frequency identification systems for management of articles within a protected area and, more specifically, to techniques for detecting unauthorized removal of articles from a protected area.

BACKGROUND

[0002] Radio-Frequency Identification (RFID) technology has become widely used in virtually every industry, including transportation, manufacturing, waste management, postal tracking, airline baggage reconciliation, and highway toll management. RFID systems are often used to prevent unauthorized removal of articles from a protected area, such as a library or retail store.

[0003] An RFID system often includes an interrogation zone or corridor located near the exit of a protected area for detection of RFID tags attached to the articles to be protected. Each tag usually includes information that uniquely identifies the article to which it is affixed. The article may be a book, a manufactured item, a vehicle, an animal or individual, or virtually any other tangible article. Additional data as required by the particular application may also be provided for the article.

[0004] To detect a tag, the RF reader outputs RF signals through the antenna to create an electromagnetic field within the interrogation corridor. The field activates tags within the corridor. In turn, the tags produce a characteristic response. In particular, once activated, the tags communicate using a pre-defined protocol, allowing the RFID reader to receive the identifying information from one or more tags in the corridor. If the communication indicates that removal of an article has not been authorized, the RFID system initiates some appropriate security action, such as sounding an audible alarm, locking an exit gate, and the like.

[0005] Most methods of determining whether articles present in the interrogation corridor have been checked out depend upon first individually detecting and identifying each tag in the field, and then checking determining the status of the articles associated with the identified tags. Some methods, for example, involve determining a serial number for each tag, and then accessing a database to determine the status of the article associated with the identified serial number. Other techniques require issuing commands to the identified tags once the serial number has been determined.

[0006] This process can be time-consuming, especially if several tags exist in the field. For example, in order to obtain a complete tag serial number, only one tag can respond at a time. If more than one tag responds at a time, a collision occurs, the data received may be invalid, and neither tag's serial number can be obtained. To deal with this, some systems use an anti-collision process, which requires each tag to respond in a different time slot until all tags are heard. This added delay is undesirable in an exit control system because patrons are in the interrogation corridor for a very short period of time. Also, each patron can be carrying multiple books. The time required to determine whether every one of the books is checked-out is often much longer than the time a patron spends in the corridor.

SUMMARY

[0007] In general, the invention relates to a Radio-Frequency Identification (RFID) system for detecting radio-frequency identification tags. More specifically, the invention relates to an RF exit control system which detects unauthorized removal of articles from a protected facility, such as books or other articles from a library. A series of antennas are set up to produce interrogation corridors located near the exit of the protected area. RFID tags are attached to the articles to be protected. In one example system, each tag includes information that uniquely identifies the article to which it is affixed and status information as to whether the article is authorized to be removed from the facility. To detect a tag, the RF reader outputs RF signals through the antennas to create an electromagnetic field within the interrogation corridor. An RF reader outputs RF power from a single port to multiple antennas via a splitter/combiner. In this way, a single RF reader with only one transmitter/receiver port simultaneously interrogates multiple antennas. The field activates the tags, and the tags, in turn, produce a characteristic response. The RF reader receives the tag information via the single transmitter/receiver port and the RF exit control system determines whether removal of the article is authorized. If removal of the article is not authorized, the exit control system initiates some appropriate security action, such as sounding an audible alarm, locking an exit gate, etc.

[0008] In one embodiment of the invention, a method comprises selectively interrogating radio frequency identification tags in an interrogation corridor such that only those tags having a selected value in a specified memory location respond to the interrogation; simultaneously receiving a response from all of the radio frequency identification tags having the selected value in the specified memory location; and detecting at least one radio frequency identification tag having the selected value in the specified memory location in the interrogation corridor if at least a partial response is received.

[0009] In another embodiment, a method comprises interrogating radio frequency identification tags in an interrogation corridor to identify presence of those tags having a selected value in a specified memory location; simultaneously receiving a response from all of the radio frequency identification tags in the interrogation corridor; detecting a collision in at least one bit of the specified memory location; and detecting at least one radio frequency

identification tag having the selected value in the specified memory location in the interrogation corridor if a collision is detected.

[0010] In another embodiment, a computer-readable medium comprises instructions that cause a processor to selectively interrogate radio frequency identification tags in an interrogation corridor such that only those tags having a selected value in a specified memory location respond to the interrogation; simultaneously receive a response from all of the radio frequency identification tags having the selected value in the specified memory location; and detect at least one radio frequency identification tag having the selected value in the specified memory location in the interrogation corridor if at least a partial response is received.

[0011] In another embodiment, a method comprises detecting a collision between communications from radio frequency identification tags in an interrogation corridor; and generating an alarm upon detecting the collision to indicate that an unauthorized article is present within the interrogation corridor.

[0012] In another embodiment, a method comprises receiving a partial response from a radio frequency identification tag in an interrogation corridor; and generating an alarm upon receiving the partial response to indicate that an unauthorized article is present within the interrogation corridor.

[0013] The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 is a block diagram illustrating a radio frequency identification (RFID) system for management of articles traveling into and out of a protected area.

[0015] FIG. 2 is a more detailed block diagram of the RF exit control system.

[0016] FIG. 3 is a graph showing the drive field signals for each of the antennas in a three-antenna RF exit control system.

[0017] FIG. 4 is a block diagram that illustrates controller in further detail.

[0018] FIG. 5 is a flow chart illustrating the overall operation of the RF exit control system.

[0019] FIG. 6 shows the frame format for communication between an RF reader and RF tags.

[0020] FIG. 7 shows two example tag signals.

[0021] FIG. 8 shows a flowchart of one embodiment of a method employed by the RF reader to determine presence of a checked-in tag in the interrogation corridor.

[0022] FIG. 9 shows an example tag signal in the presence of noise.

[0023] FIG. 10 shows another embodiment of a method employed by the RF reader to determine presence of a checked-in tag in the interrogation corridor.

[0024] FIGS. 11A and 11B show alternate embodiments of the signal strength indicator algorithm.

[0025] FIG. 12 shows another embodiment of a method employed by the RF reader to determine presence of a checked-in tag in the interrogation corridor.

[0026] FIG. 13 shows another embodiment of a method employed by the RF reader to determine presence of a checked-in tag in the interrogation corridor.

[0027] FIG. 14 shows embodiment of a method employed by the RF reader to determine presence of a checked-in tag in the interrogation corridor.

DETAILED DESCRIPTION

[0028] In general, techniques are described herein for detecting Radio-Frequency Identification (RFID) tags. More specifically, this description is directed to techniques that utilize an RF exit control system to detect unauthorized removal of articles from a protected area. The protected area is generally of the type in which the removal of articles must be authorized, such as books in a library or items in a retail store. Each article in the facility contains an RFID tag, which may uniquely identify the article to which it is affixed. In addition, for purposes of the present description, the RFID tag also contains status information indicating whether removal of the article is authorized. The RFID tag may be embedded within the article so that the tag is substantially imperceptible, to help prevent tampering. An exit control system determines if removal of the article from the facility has been authorized (e.g., a book has been properly checked-out by a library patron or staff member) and sets off an alarm if it has not.

[0029] FIG. 1 is a block diagram illustrating a radio frequency identification (RFID) system 10. Exit control system 5 detects unauthorized removal of articles from a protected area 7. For purposes of the present description, the protected area will be assumed to be a library and the articles will be assumed to be books or other articles to be checked out. Although the system will be described with respect to detecting checked-in tags to prevent their unauthorized removal from a facility, it shall be understood that the present invention is not limited in this respect, and that the techniques described herein are not dependent upon the particular application in which the RFID system is used. For example, the system could also be used to check for other kinds of status or type information without departing from the scope of the present invention.

[0030] Exit control system 5 includes lattices 9A and 9B which define an interrogation zone or corridor located near the exit of protected area 7. The lattices 9A and 9B include antennas for interrogating the RFID tags as they pass through the corridor to determine whether removal of the item to which the tag is attached is authorized. As described in further detail below, exit control system 5 utilizes a single reader to drive multiple antennas. To detect a tag, an RF reader outputs RF power through the antennas to create an electromagnetic field within the interrogation corridor. The RF reader outputs RF power from a single port to multiple antennas via a splitter/combiner. In this way, a single RF reader with only one transmitter/receiver port simultaneously interrogates the corridor using multiple antennas. The field activates the tags and the tags, in turn, produce a characteristic response. The RF reader receives the tag information via the single transmitter/receiver port and the exit control system determines whether removal of the article is authorized. If removal of the article is not authorized, the exit control system initiates some appropriate security action, such as sounding an audible alarm, locking an exit gate, etc.

[0031] In addition, the overall RFID system 10 may include a number of "smart storage areas" 12 within protected area 7. For example, an open shelf 12A, a smart cart 12C, a desktop reader 12E and other areas. Each smart storage area 12 includes tag interrogation capability which enables tracking of articles throughout a facility. In a library setting, for example, a book could be tracked after check-in while en route to a shelf 12A on a smart cart 12C.

[0032] The RFID tags themselves may take any number of forms without departing from the scope of the present invention. Examples of commercially available RFID tags include 3M™ RFID tags available from 3M Company, St. Paul, MN, or "Tag-it" RFID transponders available from Texas Instruments, Dallas, TX. An RFID tag typically includes an integrated circuit operatively connected to an antenna that receives RF energy from a source and backscatters RF energy in a manner well known in the art. The backscattered RF energy provides a signal that may be received by an interrogator within RFID system 10 to obtain information about the RFID tag, and its associated article.

[0033] An article management system 14 provides a centralized database of the tag information for each article in the facility. Article management system 14 may be networked or otherwise coupled to one or more computers so that individuals, such as a librarian, at various locations, can access data relative to those items. For example, a user may request the location and status of a particular article, such as a book. Article management system 14 may retrieve the article information from a database, and report to the user the last location at which the article was located within one of the smart storage areas. Optionally, the system can re-poll or otherwise re-acquire the current location of the article to verify that the article is in the location indicated in the database.

[0034] FIG. 2 shows a more detailed block diagram of an example embodiment of the RFID exit control system 5. As illustrated, exit control system 5 is configured for transmitting and/or receiving data from one port of RF reader 20 to/from multiple antennas according to the techniques described herein.

[0035] More specifically, exit control system 5 includes antennas 8A, 8B and 8C (collectively referred to as "antennas 8") positioned to provide multiple interrogation zones 40A and 40B. Each antenna 8A-C includes an associated tuner 18A-C through which the antennas are connected to RF reader 20 and ultimately to controller 14. Although FIG. 2 shows system 10 as including three antennas 8A-8C and two interrogation zones 40A and 40B, it shall be understood that exit control system 5 can include any number of antennas set to provide any number of interrogation zones depending upon the needs of the facility.

[0036] Exit control system 5 operates within a frequency range of the electromagnetic spectrum, such as 13.56 MHz, with an allowable frequency variance of +/- 7 kHz, which is often used for Industrial, Scientific and Medical (ISM) applications. However, other frequencies may be used for RFID applications, and the invention is not so limited.

[0037] Antennas 8 may be designed to develop electromagnetic fields of at least certain strengths within the interrogation corridors 40. This may be advantageous for one or more reasons, including improving the likelihood of detecting tags having the desired status, e.g., tags that are checked-in in a library application. In one embodiment, the electromagnetic fields created by the antennas 8 are used to power the RF tags in the corridors 40. The amount of energy induced in each RF tag is proportional to the strength of the magnetic field passing through the tag loop. The antennas 8 therefore may produce a field having a magnitude that exceeds a threshold magnitude for energizing an RF tag, such as 115dBuA/m. In addition, the magnitude preferably meets or exceeds the threshold magnitude throughout a substantial volume of the interrogation corridor. For example, the field produced may have a magnitude that exceeds the threshold magnitude for 50%, 75%, 90%, 99%, or more of the volume of the interrogation corridor, thus increasing the likelihood that unauthorized (i.e., tags that are still checked-in) RF tags in the corridor are successfully detected.

[0038] The RF Reader 20 of exit control system 5 may also read/write data from/to the RFID tags. RF reader 20 outputs RF power from one transmitter/receiver port 21 to multiple antennas 8 via a splitter/combiner 42. In this way, one RF reader 20 with only one transmitter/receiver port 21 can simultaneously use multiple antennas to interrogate RF tags. In the embodiment shown in FIG. 2, the splitter/combiner 42 is external to RF reader 20 such that the system is easily scalable. Thus, to accommodate a different number of interrogating antennas, only the splitter/combiner 42 need be changed.

[0039] RF reader 20 receives a response from the RFID tags through the same splitter/combiner 42 and transmitter/receiver port 21. The received signal is analyzed by the system to determine whether a checked-in (e.g., not checked out) article is present in an interrogation corridor 40.

[0040] By providing RF power to each antenna with RF reader 20, each antenna 8 receives RF power and none of the antennas 8 need rely on electromagnetic coupling to a driven antenna to get power. This greatly improves the detection capability of the exit control system 5 under conditions where electromagnetic coupling is inadequate, such as when the antennas are not large enough or close enough together to allow efficient coupling.

[0041] Because RF reader 20 receives a response from the RFID tags through the same splitter/combiner 42, the return signal from any RF tags in the corridor are combined going back through the splitter/combiner 42 into the RF reader transmitter/receiver port 21. In this way, if a weak tag signal is received by antenna 8A and a weak signal for the same tag is also received by antenna 8B, for example, the two weak signals from antennas 8A and 8B are combined at splitter/combiner 42. The combined signal is then input into RF reader 20 through transmitter/receiver port 21. This greatly increases the likelihood detecting even weak tag signals.

[0042] In an example embodiment, the exit control system 5 detects only whether at least one checked-in tag is present in the corridor. There are several situations in which numerous tags could be present in the corridor. For example, one patron could be carrying multiple articles through the corridor. Alternatively, multiple patrons, each carrying at least one article, could pass through the same or different corridors simultaneously. Furthermore, because of the relatively short period of time it takes for a patron to pass through the corridor, there typically is not enough time to receive and analyze individual information for each and every tag that may be in the corridor. By combining the individual signals from each of the antennas in the system, the signal received by the RF reader will indicate simply whether at least one checked-in tag is present in the corridor. The present exit control system is thus designed such that even when numerous tags are present in the corridor, if at least one of them has checked-in status, the system will alarm. Similarly, when numerous tags are present in the corridor and more than one of them has checked-in status, the system will alarm. The librarian or other designated employee can then check the articles to determine which of the articles present when the system alarmed have not been properly checked-out. The methods by which the system may determine presence of a checked-in tag (i.e., one that has not been properly checked-out and is therefore not authorized to be removed from the facility) are described in further detail below with respect to FIGS. 7-14. Although the system is described with respect to detecting presence of checked-in tags to prevent their unauthorized removal from a facility, it shall be understood that the present invention is not limited in this respect. For example, the system could also be used to check for other kinds of status or type information without departing from the scope of the present invention.

[0043] Photocells 24A and 24B, one for each interrogation corridor 40A and 40B, respectively, signal presence of a patron in their respective corridors. Interconnects 16A, 16B and 16C connect the alarms 12 and photocells 24 to controller 14. A counter 22 may also be included which increments each time one of photocells 24 detect a patron in the corridor.

[0044] In one embodiment, each antenna 8 nominally receives the same amount of RF power from RF reader 20, but, as will be described in more detail below, is driven ninety degrees out of phase with its neighboring antennas. The phase shift, by creating a rotating field between antennas, enhances the ability of the system to detect tags regardless of the orientation of the tag. In this manner, the exit control system 5 transmits and receives from one RF reader transmitter/receiver port 21 to multiple antennas 8 via a splitter/combiner 42. Antennas 8 receive nominally the same amount of power from the RF reader, but are driven 90° out of phase with each other.

[0045] In one embodiment in which a response is received for a checked-in tag, the RF reader 20 communicates with the controller 14, which may enable alarms 12. In FIG. 2, alarms 12 include visual alarms 12A and 12C and audible alarm 12B, although any combination of visual, audible, or other method of communicating checked-in RF tag presence may be used.

[0046] FIG. 3 is a graph that shows the resulting phase shift of the RF drive signals 43A-C for each antenna 8A-8C (FIG. 2), respectively. As shown in FIG. 3, the RF drive signal 43B for antenna 8B is 90° out of phase with the RF drive signal 43A for antenna 8A; the RF drive signal 43C for antenna 8C is 180° out of phase with antenna 8A, etc.

[0047] The phase shift allows the system to detect RF tags in all orientations by creating a rotating field between the antennas. Thus, regardless of the orientation of the RF tag as it travels through the interrogation corridor, the likelihood of detection is increased.

[0048] Various methods can be used to achieve the 90° phase shift between neighboring antennas. In one embodiment, the antennas are connected using transmission lines that differ by ¼ wavelength between neighboring antennas to achieve the desired 90° phase shift. For example, referring again to FIG. 2, lines 32A, 32B and 32C which connect the antennas 8A, 8B and 8C to splitter/combiner 42 could be implemented by coupling lengths of ¼ wave transmission lines as appropriate to drive each successive antenna 90° out of phase as shown in FIG. 3.

[0049] In another embodiment, compensation circuitry could be provided at each antenna 8A-C to adjust the phase shift induced by transmission lines 32A-C such that the resulting phase shifts are 90° out of phase as shown in FIG. 3.

[0050] The exit control system 5 thus provides several advantages. One RF reader with only one transmit/receive port can be used to simultaneously utilize multiple antennas. By providing RF power to each antenna at a controlled amplitude and phase, magnetic coupling is not relied upon to deliver power to the antennas and to control the relative phase of each antenna. Also, because the interrogating fields are driven to produce a rotating interrogation field, coverage is increased in the interrogation corridor. In addition, the system is scalable – namely, the number of interrogating antennas to be utilized in any particular system can be accommodated by changing only the RF splitter. Weak signals from multiple antennas are combined to form an adequate signal, thus also increasing the likelihood of detecting signals. Moreover, EM emissions are reduced by driving the antennas at a 90° phase shift, as the far fields for any antennas driven 180° apart will cancel.

[0051] FIG. 4 is a block diagram that illustrates controller 14 in further detail. As illustrated, in the embodiment depicted in Figure 2, controller 14 receives an input signal 45 from interconnect 16A that indicates a patron has been detected in corridors 40. In addition, controller 14 receives an input signal 47 from RF reader 20 that indicates that the RF reader has detected at least one signal within corridors 40In an embodiment, as described in further detail below, controller 14 continually monitors input signals 45 and 47. When input signals 45 and 47 indicate that both a patron and a checked-in tag have been detected, controller 14 initiates an alarm.

[0052] FIG. 5 is a flowchart 50 further illustrating exemplary operation of controller 14. As illustrated, controller 14 performs a continuous loop monitoring that looks for a checked-in tag in the corridor, or for a patron to enter the corridor, and initiates an alarm only when both a patron and a checked-in RF tag are detected in an interrogation corridor. Thus, controller 14 continually monitors input signals 45 and 47 to determine whether a checked-in RF tag (52) or a patron (54) is present in any of corridors 40A or 40B. If either one of these conditions is met, controller 14 starts a timer (56 or 58, respectively). The purpose of the timer is to ensure presence of both a patron and a checked-in RF tag in the corridor at essentially the same time, for example, within 0.5 seconds, or some other time as may be appropriate.

[0053] Controller 14 next determines whether the other criteria, namely either a patron (60) or a checked-in RF tag (62) is present. If not, controller 14 checks whether the timer has timed out (64 or 66, respectively). If so, then both a patron and a checked-in RF tag were not present within the allotted time frame, and controller 14 returns to the beginning of the loop.

In the event that both a patron and a checked-in tag are present in the corridor within the allotted time frame, controller 14 activates the alarm (68).

[0054] Various techniques by which the exit control system determines whether an unauthorized tag is present in the corridor will now be described. In one embodiment, the techniques described herein allow RF reader 20 to quickly determine whether any articles that are not properly checked-out (in other words, articles that have checked-in status and are therefore not authorized to be removed from the facility) are in the interrogation corridor. The techniques allow RF reader 20 to rapidly and accurately determine the presence of articles with checked-in status in the corridor, and will minimizes the adverse impact of tag collisions that may otherwise degrade the system performance.

[0055] As described above, quickly determining the presence of a tag with checked-in status can be important because of the relatively short period of time in which each patron is in the interrogation corridor, and the fact that multiple patrons can be in the interrogation corridor at the same time. The present techniques described below enable this in several ways. First, RF reader 20 does not necessarily require receipt of a full tag serial number for each tag in the corridor in order to determine the status of the tag. For example, in some embodiments, all of the checked-in tags in the corridor may respond at the same time. In other words, the techniques do not necessarily require that each tag in the corridor respond in a separate time slot so that each tag can be individually identified. In fact, in some embodiments, there is no need to even individually identify each tag in the corridor to determine the status of the tags. In some embodiments described below, the transmission of a complete, single communication frame is not required.

[0056] RF reader 20 and the RF tags communicate using a known protocol in which each message is embedded within one or more frames of a predefined format. The format of an example RFID transmission frame 100 is shown in FIG. 6. The frame 100 includes a start of frame (SOF) 102, a message 104, cyclical redundancy check (CRC) 106 and end of file (EOF) 108. SOF 102 indicates the beginning of the frame. Similarly, EOF 108 indicates that the entire frame has been transmitted. Any non-fixed data is embedded in the message 104 portion of the frame 100 and CRC 106 reflects the data in the message 104.

[0057] CRC 106 is used to check the integrity of the data. To calculate CRC 106, all bits of the data are pushed through a predetermined algorithm. Once the frame is transmitted, the receiver decodes CRC 106 using the received data to determine whether the message 104 was properly transmitted. If the CRC generated from the received data does not match the CRC contained within the frame itself, an error occurred.

[0058] One aspect of the presently described techniques is directed to ensuring that only tags that are not checked-out (i.e., still checked-in) respond when passing through the interrogation corridor. This can be accomplished by making use of a feature called the Application Family Identifier (AFI) byte. This feature is described in the ISO 15693 standard for RFID systems. The AFI byte is a piece of memory in the RFID tag that contains one 8-bit value. The AFI is normally used to identify the type of article to which the tag is attached, such as book, CD, videotape, etc. The value stored in the AFI location can be changed through a defined series of commands described in the ISO 15693 standard. When the RF reader issues an AFI command it sends an AFI value. As defined in the ISO 15693 standard, when the AFI value transmitted in a command is 0x00 (hexadecimal) then all tags in the interrogation field respond. When the RF reader transmits any value other than 0x00, then only tags with a matching AFI value in memory respond to the command.

[0059] The techniques described herein use the AFI byte to indicate the status of the article, for example, whether the article has been checked-out. The AFI field is therefore used as a checked-in/checked-out status byte. When books or other articles are on the shelf the AFI byte is set to a designated "checked-in" value. When a librarian checks out the book or a patron checks out at a self check station the AFI value is changed to a different, "checked-out" value.

[0060] The RF reader scans for tags containing the checked-in value in their AFI memory location. This will cause all tags with their AFI byte set to "checked-in" to respond. If the RF reader receives a response from the tags then the item was not properly checked-out. This is because any item that was properly checked-out would not have the checked-in value in their AFI byte and would not respond.

[0061] An example of how the present technique of using the AFI byte as a checked-in/checked-out status byte will now be described. A patron returns an item to an automatic book drop. The book drop reads the serial number and sets the AFI byte to "checked-in". The item is returned to the shelf and then another patron decides to leave with the item. The new patron inadvertently leaves without checking-out the book. The patron walks through the interrogation corridor, which is looking for tags having the "checked-in" value. When the system sees the checked-in tag in the corridor, the system will alarm.

[0062] If instead the patron properly checks-out the item, the AFI byte is set to "checked-out". When the patron passes through the corridor, the tag will not respond to the system's command because the system asks only checked-in tags to respond. The patron can thus walk through the corridor and remove the article without alarm.

[0063] A second technique described herein is directed at verifying that the received tag communication is actually a tag-produced response and not noise-produced. Namely, in one embodiment, the system asks all tags in the interrogation field to respond at the same time. Under normal circumstances this would only be done in a situation where one tag was present in the field at a time. When two or more tags respond in the same timeslot it creates a situation called a "collision". Normally when a collision occurs, no message 104 of the responding tags can be heard properly. In many systems, a process called anti-collision is implemented and tags are commanded to respond in different timeslots until all tags are identified. However, this process typically consumes too much time in exit control applications, in which tags pass quickly through the corridor.

[0064] Instead, the techniques described herein ask all tags to respond in the same time slot knowing that collisions will occur if more than one unchecked-out (checked-in) tag is present in the corridor. This embodiment makes use of the fact that the SOF is one piece of information that can still be validly received even when collisions occur. The SOF is the first transmission sent by tags responding to a command. Regardless of how many tags respond to the command they will all respond with the same SOF at the same time. By detecting the SOF, the system validates that at least one checked-in tag is actually in the interrogation field.

[0065] FIG. 7 shows an example of two tag signals, a first tag signal 110 and a second tag signal 112. Both signals 110 and 112 transmit the same SOF, but have different data in the message fields. Since both tags are responding at the same time and the data is combined by the splitter/combiner going back into RF reader, the data in the message field received by the RF reader is subject to a collision. The SOF, however, does not collide irrespective of how many tags are in the field.

[0066] FIG. 8 is a flowchart 130 of the present technique for verifying presence of an unchecked tag in an interrogation corridor using the AFI byte as a status byte and the SOF as verification that an unchecked tag is in the field. First, the RF reader sends the AFI command with the AFI value set to checked-in (134). Each tag with a matching checked-in AFI byte responds, and the possible checked-in tag response is received (136). Next, to verify that the response is an actual tag response and was not created by noise, the system checks for the SOF (138). If a valid SOF was received, at least one checked-in tag is present in the interrogation corridor (140) and the alarm is activated (142). The alarm is activated for a predetermined duration. On the other hand, if a valid SOF is not received, the system assumes that noise caused the response, and that therefore there is not a checked-in tag in the corridor (146). The loop then restarts by sending an AFI command (134).

[0067] In other embodiments techniques to ensure the validity of the SOF are used. In particular, a received signal strength indicator is used to separate actual tag-produced responses from noise-produced responses. FIG. 9 shows an example of tag signal frame in the presence of noise. The tag signal 114 is shown on top of a noise floor 120. This noise floor is measured and analyzed as described below to verify a valid SOF.

[0068] FIG. 10 is a flowchart 170 showing this technique. FIG. 10 is similar to FIG. 8 in that the AFI byte is used as a checked-in/checked-out status byte and the SOF is used to validate a tag-produced signal. In addition, the flowchart of FIG. 10 uses a received signal strength technique to validate the SOF. First, the AFI command is sent with the AFI byte set to checked-in (166). Then, the noise floor of the corridor is measured (164) prior to any tag response. Any tag with AFI byte set to checked-in will respond to the command, the response is received and the signal strength is measured (168). The system next checks for the SOF (170). If a SOF is detected, the response signal strength is compared with the noise floor (172). This is because although receipt of an SOF is an indication that a tag is in the field, since the SOF is only 8-bits long noise can sometimes produce an SOF sequence. If the differential between the response signal strength and the noise floor is adequate to indicate that the signal is authentic (174), the system validates that a checked-in tag is present in the interrogation field (176). The system then alarms (178). On the other hand, if the differential is not adequate (174), the system assumes that noise created the response and that therefore there is no checked-in tag in the corridor (182). The loop is then restarted.

[0069] FIGS. 11A and 11B show two embodiments of the method for comparing the possible received tag response with the noise floor (172 in FIG. 10). In FIG. 11A, method 172A first looks for a difference between the measured noise floor and the measured signal strength, the signal strength measurement occurring during the time of the signal response period, that is adequate to indicate that the received signal is authentic (202). If the signal strength differential is adequate to indicate that the signal is authentic (204), the RF reader indicates that an unchecked-out (i.e., checked-in) tag is present in the corridor (208). If the signal strength differential is not adequate to indicate that the received signal is authentic, the RF reader assumes that noise produced the response and that therefore no checked-in tags are present in the corridor (206).

[0070] In FIG.11B, the method not only looks at the noise floor before the SOF, but also after the end of the expected tag response. Checking the noise floor after the EOF is received is one more verification that the response was really a tag-produced response and not a noise-produced response. The method 172B first looks for a differential between the noise floor measured prior to the SOF and the signal strength (220). If the differential is not adequate to indicate that the signal is authentic (222), the system assumes a noise-produced response and signals that no checked-in tags are present in the corridor (226). If the differential is adequate, (222), the system next looks for a differential between the signal strength and the noise floor measured after the EOF of the expected tag response (228). If this differential is also adequate (230), the system signals that a checked-in tag is present in the corridor (232).

[0071] The techniques described in FIGS. 10 and 11 may have several advantages. By having all the tags respond in the same time slot, the amount of time required to determine whether a checked-in tag is present in the interrogation field is significantly reduced. The minimum scan time is reduced from around 60ms to around 20ms. In addition, when all the checked-in tags respond at the same time, the likelihood of detecting a checked-in tag is increased because the signals are combined going back into the RF receiver. Also, since the system only looks for the SOF, the whole tag transmission need not be heard to determine whether or not it is checked-in. This can occur when a tag moves into a weaker portion of the interrogation field and loses power half way through the transmission. In this way, the system can reliably alarm even if a tag only has enough power to transmit part of its serial number. In fact, the checked-in tag need only transmit its SOF for the system to detect its presence. Furthermore, the system is not compromised when multiple tags respond at the same time. In fact, the system is designed so that this is the case. Multiple tag responses occurring at the same time actually increase the likelihood that a checked-in tag will be detected.

[0072] The signal strength indicator can be implemented using a variety of embodiments. In one embodiment, the signal strength indicator is generated by a circuit, and provides an indication of the strength of the received signal. This information is amplified and sent to the controller (reference numeral 14 in FIG. 2). The controller 14 uses an analog-to-digital converter to analyze the signal as described above with respect to FIGS. 11A and 11B.

[0073] FIG. 12 shows another embodiment of a method by which the RF reader may determine whether a checked-in tag is present in the interrogation corridor. This process (250) is used with the "Tag-it" type tags available from Texas Instruments as mentioned above. There is a command in the Tag-it protocol where all tags in the interrogation field respond with the data stored in an defined block and they will all respond at the same time. The present technique sets one block of data in the tag as the "check-out status block." The command is then used to determine whether at least one unchecked-out (checked-in) tag is in the field.

[0074] For example, assume the check-out status block in a checked out book is set to:

00000001

and the data in a checked-in book is set to:

00000000.

[0075] As tags move through the interrogation field, the "read unaddressed block" command is sent by the RF reader. Every tag in the field will respond at the same time. As the tags respond the RF reader will receive the SOF as described above. The check-out status block for each tag will be identical except for the last bit and the CRC if both checked-out and checked-in tags are present. The present method checks for collisions on the last bit of the check-out status block and the CRC to determine whether at least one checked-in tag is present in the interrogation field. For example, the following table shows the possibilities that may occur, where "clear" indicates no collision was detected.

All checked-out books	SOF – clear	No alarm

	Checked-out status – clear CRC – clear	
All checked-in books	SOF – clear Checked-out status – clear CRC – clear	Alarm
Both checked-out and Checked-in books	SOF – clear Checked-out status – collision on last bit CRC – collisions	Alarm

[0076] In reference to FIG. 12, the RF reader sends the "read unaddressed block" command (252). The possible tag response is received (254). The system checks for SOF using the techniques described above with respect to FIG. 8, 10 and/or 11. If the SOF is not detected (256), the reader continues checking (252). If an SOF was detected, the system checks for a collision on the last bit of the checked-out status byte (258). If a collision is detected (260) the reader next checks the CRC (262). If a collision is detected in the CRC the system signals that at least one checked-in tag is in the corridor (264) and activates the alarm (266). This is the situation shown in row three of the Table discussed above.

[0077] If no collision occurred in the checked-out status bit (260) the reader determines whether the checked-out status bit is set to checked-in (268). If so, the reader checks for collisions in the CRC (270). If there are no collisions, then all of the tags in the corridor are checked-in tags (272) and the controller activates the alarm (266). This is the situation shown in row two of the Table shown above.

[0078] If no collision occurred in the checked-out status bit (260) and the checked out status bit is not checked-in, then the books must be checked-out, there are no checked-in tags in the corridor (274) and the next response is checked (276). This is the situation shown in row one of the Table shown above.

[0079] Other embodiments may also be used to determine presence of a checked-in tag in the interrogation corridor. One of these embodiments is shown in FIG. 13. The flowchart may depict an algorithm that runs continuously in the RF reader. When the RF reader indicates an alarm (320) a message is sent to the controller notifying that a checked-in book has passed through the interrogation corridor. This algorithm shown in FIG. 13 ignores collisions and overpowered tags during the first sweep for tags. The algorithm concentrates on reading as many tags as possible as quickly as possible.

[0080] The algorithm shown in FIG. 13 allows the current TI "Tag-it" and TI ISO 15693-3 tags to be used in an exit control system without significant degradation of performance. One conventional way to determine whether the TI-type tags are checked-in is to run a SID (Simultaneous IDentification) Poll on all tags in the field and then read from the specific block where the checked-in/checked-out code is kept. One potential problem with this technique is that the SID Poll will continue until all collisions are resolved (when multiple tags talk at the same time) and if one tag leaves the field during this algorithm, then the process halts and no data is returned. This could very easily happen in a detection environment where tags are constantly moving into and leaving the field - patrons walking through the exit control system with books (which have tags).

[0081] The algorithm shown in FIG. 13 uses a modified SID poll (302) and tries to resolve as many tags as possible as quickly as possible the first time through the algorithm (304 and 310). If a tag with a set checked-in code is found (312), the alarm is triggered (320). If there is still time remaining (304) (the tags are still in the field), then the algorithm will attempt to resolve as many collisions as possible (308). Because it only issues the unmasked SID poll and ignores collisions unless there is enough time to resolve them, the speed with which the algorithm can identify unchecked-out tags in the field is increased.

[0082] The statistics for this method are described below. The first set of numbers given in parentheses are examples of least significant digits of the SID code. This is based on the 16 timeslot SID algorithm. The second set of numbers in parenthesis is the number of tags validated after the first pass.

0 Tags 100.00%

1 Tag 100.00%

2 Tags: 15/16 chance of reading 93.75%

3 Tags: No Collisions (012) 210/256 chance (82.03%)
One Collision (011) 45/256 chance (17.57%)
Two Collisions (111) 1/256 chance (0.39%)
Overall Chance:
No Collisions + 1/3 * One Collision + 0 * Two Collisions 87.89%

4 Tags: No Collisions (0123) 2730/4096 chance (66.65%)
One Collision (0012) 1260/4096 chance (30.76%)
Two Collisions (0001) 60/4096 chance (1.46%)

Double Collision (0011) 45/4096 chance (1.10%)
Three Collisions (0000) 1/4096 chance (0.02%)
Overall Chance:
No + 1/2 One + 1/4 Two + 0 Double + 0 Three 82.31%

5 Tags: No Collisions (01234) 32760/65536 (49.99%)
One Collision (00123) 27300/65536 (41.66%)
Two Collisions (00012) 2145/65536 (3.27%)
Three Collisions (00001) 1290/65536 (1.97%)
Four Collisions (00000) 1/65536 (0.00%)
Two / Two (00122) 1890/65536 (2.88%)
Two / Three (00111) 150/65536 (0.22%)
Overall Chance:
No + 3/5 One + 2/5 Two + 1/5 Three + 1/5 2-2 77.26%

[0083] It shall be noted that with 3 tags, if there are no collisions, all tags will be verified. If there is one collision, the colliding tags will not be read, but the one tag which does not match will be read, and since this is one of the three possible tags, a factor of 1/3 is used to multiply by the percentage chance of having one collision. This logic is continued throughout the other 4 and 5 tag statistics. It shall also be understood that these percentages are only for the first pass, and the other tags will be resolved on subsequent passes, time and location of the tags permitting.

[0084] Another embodiment of the checked-in tag detection is shown in FIG. 14. The algorithm refers to a database containing tag ID's of properly checked out items. This database that may reside on the exit control system itself, but the invention is not limited in this way.

[0085] First, an SIF poll is performed on the tags in the interrogation corridor (352). When tags are detected in the interrogation fields (354), the algorithm only gathers the tag ID's that can be resolved before the tags leave the interrogation corridor (360). The amount of time before a tag leaves the interrogation corridor could either be determined as an average calculated value based upon expected speed through the portal or be dynamically determined by the inventory of tags being collected.

[0086] An additional poll of tags could also be required after each collision is resolved. If this poll doesn't get a least one duplicate tag ID as that was obtained in the initial poll, the determination could be that a new set of tags has entered the interrogation corridor. This would trigger the database query for the previous set of tags.

[0087] Another possible strategy would be to infer that the tag has left the corridor as soon as the current collision cannot be resolved. This also would trigger the database query.

[0088] The algorithm shown in FIG. 14 thus specifically focuses on collecting as many tag ID's as possible and does not check for security information until the above mentioned time is expired. At that time, a query is made to the database to determine if all the detected tags exist in the security database.

[0089] The advantages provided by the embodiment of FIG. 14 are related to the effects of non-uniform fields, as well as the amount of time available for tag detection. This algorithm provides a means of maximizing the number of tags to sample for security. This algorithm is not affected as significantly by non-uniform fields because once the tag ID is collected, the system no longer needs to communicate with the tag for security information.

[0090] The following discussion is directed toward a method for use with the new Electronic Product Code (EPC). The EPC is set to supplant the Universal Product Code (UPC) in certain applications by using RFID for item identification. Within this new specification is a "destroy" command that when executed renders the RFID tag destroyed or nonfunctional. The method creates a "key" for this destroy command which is difficult to detect as well as secure so that malicious use of the destroy command will not affect performance of the RFID tag.

[0091] The destroy command renders the RFID tag nonfunctional. To set the destroy code, a proper command is given to the chip and the memory is programmed. To execute the destroy command, the password which was placed in the destroy memory location must be sent again to the chip, and if there is a match then the chip is destroyed.

[0092] The present method creates a secure "key" for the destruction of RFID tags. If one key was used for all tags at all locations, if someone were to break the key, they could in theory destroy all RFID at that location. For example:

	Tag A	Tag B	Tag C
Destroy Code:	G	G	G

[0093] The same code in the destroy register yields a possibility of compromising all tags in an installation.

[0094] With the present method, however, the EPC identification code (up to 88 bits of information) is run through an algorithm and further placed into the destroy memory register (24 bits). This would make every destroy command unique to each tag, and would make a unique key that is difficult to decipher. For example:

	Tag A	Tag B	Tag C
Destroy Code:	U	W	L

[0095] An algorithm "key" is common to all tags and destroy codes, but because the destroy code cannot be read from the tags, the presently described method makes it much more difficult to break the algorithm, thus maintaining the overall security of the site.

Example EPC Identification:	00000000	00 hex
	11111111	FF
	00000000	00
	11111111	FF
	00000000	00
	11111111	FF
	00000000	00
	11111111	FF
	00000000	00
	11111111	FF
	00000000	00

88 bits organized into 11 blocks of 8 bits.

[0096] An example algorithm may, for example, select some memory, perform a function (add, subtract, multiply with data or constants, etc.) and create an output destroy command.

Destroy command	10001101	8D
(random for this example)	01111011	7B
	00010110	16

[0097] Another EPC value with this algorithm run would create an entirely different destroy command value.

[0098] Between sites, a different algorithm could be used to discern different stores or vendors such that the different algorithm would not allow the tags to be destroyed. In a shipping security example, only articles sold to one retailer to could be sold by that same retailer. Between two stores with different algorithms, the identical EPC value would yield a different destroy command code.

[0099] Various embodiments of the invention have been described. These and other embodiments are within the scope of the following claims.